

**Міністерство освіти і науки України
Рівненський державний гуманітарний університет**



МАТЕРІАЛИ
IX Всеукраїнської
науково-практичної конференції
„ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В
ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ»

25 березня 2015 року
м. Рівне

ББК 32.973.2-018
УДК 004
І-74

**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРОФЕСІЙНІЙ
ДІЯЛЬНОСТІ: Матеріали ІХ Всеукраїнської науково-
практичної конференції.- Рівне: РВВ РДГУ.- 2015.- 222 с.**

Програмний комітет:

Постоловський Р.М., канд.іст.наук, професор, ректор Рівненського державного гуманітарного університету

Поніманська Т.І., канд.пед.наук, професор, проректор з наукової роботи Рівненського державного гуманітарного університету

Сяський А.О., докт.техн.наук, професор кафедри інформатики та прикладної математики Рівненського державного гуманітарного університету

Шахрайчук М.І., канд. фіз.-мат. наук, доцент, декан факультету математики і інформатики Рівненського державного гуманітарного університету

Батишкіна Ю.В., канд.техн.наук, доцент, завідувач кафедри інформаційно-комунікаційних технологій та методики викладання інформатики Рівненського державного гуманітарного університету

Войтович І.С., докт.пед.наук, професор кафедри інформаційно-комунікаційних технологій та методики викладання інформатики Рівненського державного гуманітарного університету

Рекомендовано до друку Вченою радою Рівненського державного гуманітарного університету (протокол №3 від 27.03.2015 р.)

загальних питань теорії і практики системного дослідження об'єктів за допомогою інформаційних машин, методів прийняття рішень за допомогою кібернетичних систем та особливостей побудови їх моделей.

Таким чином, в першу чергу необхідним є визначення місця інформаційних машин у технічних системах згідно теорії механізмів і машин, а саме загальної класифікації типів машин та розкриття їх видів і принципів застосування (рис.1). Крім того, студенти повинні бути ознайомлені із основними методами системного аналізу.



Рис.1. Загальна класифікація типів машин

Для того, щоб оволодіти знаннями щодо принципів застосування математичних машин, які перетворюють вхідну інформацію в математичну модель досліджуваного об'єкта передбачено, зокрема, вивчення основних статистичних функцій та їх використання у процесі обробки експериментальних даних в середовищі MS Excel (визначення лінії тренду, оцінка адекватності отриманої математичної моделі, прогнозні значення).

З метою опанування студентами основ застосування кібернетичних систем доцільним є вивчення принципів управління на базі нечіткої логіки [2]. Теорія нечіткого керування є однією з гілок теорії інтелектуальних систем і активно застосовується в даний час для синтезу нечітких регуляторів, гібридних регуляторів, нечітких пристроїв оцінювання і фільтрації. Нечіткі системи в порівнянні з традиційними мають кращу перешкодозахищеність, швидкодію і точність за рахунок більш адекватного опису реального середовища, в якому вони функціонують [3].

Варто відзначити, що специфікою дисципліни «Інформаційні машини і кібернетичні системи» є те, що вона охоплює великий об'єм матеріалу і викладається для студентів напрямку підготовки «Технологічна освіта», які володіють тільки базовими знаннями в області комп'ютерних технологій. Тому доцільним є доповнення курсу відеоматеріалами з описом створених прикладних кібернетичних систем (наприклад, пральних машин з інтелектуальним керуванням чи деревообробних станків з числовим програмним керуванням).

Отримані знання щодо принципів системного дослідження об'єктів за допомогою інформаційних машин, методів застосування кібернетичних систем дозволяють набути вмінь виконувати системний опис об'єкту аналізу, обґрунтовано вибирати методи застосування інформаційних машин для раціонального розв'язання конкретних прикладних задач.

Список використаних джерел

1. Пальчевський Б. О. Дослідження технологічних систем (моделювання, проектування, оптимізація): навч. пос. / Б. О. Пальчевський. – Львів: Світ, 2001. – 232 с.
2. Лозинський А. О. Системи керування електропобутовими приладами: навч. пос. / А. О. Лозинський, Б. Л. Копчак. – Львів: видавництво Національного університету “Львівська політехніка”, 2009. – 224 с.
3. Рубанов В.Г. Интеллектуальные системы автоматического управления. Нечеткое управление в технических системах: учеб. пособие / В. Г. Рубанов, А. Г. Филатов. – БГТУ им. В. Г. Шухова, 2010. – 170 с.

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБИГУ НА ОСНОВІ СИСТЕМ ІДЕНТИФІКАЦІЇ

Кошева Наталія Анатоліївна, кандидат технічних наук, доцент кафедри інформатики та ОТ
 Мазниченко Наталя Іванівна, старший викладач кафедри інформатики та ОТ
 Національний юридичний університет ім. Ярослава Мудрого

Розглянуті та проаналізовані переваги та недоліки сучасних підходів щодо захисту документів в системах електронного документообігу за рахунок використання систем ідентифікації користувачів.

Ключові слова: інформаційна безпека, ідентифікація користувачів комп'ютерних систем

Considered and the analyses advantages and lacks of modern approaches in relation to security of documents in the systems of electronic circulation of documents due to the use of the systems of authentication of users.

Keywords: informative safety, authentication of users of the computer systems

У багатьох сферах діяльності широке розповсюдження одержало використання електронних документів. Використання систем електронного документообігу (СЕД) дозволяє досягти величезного економічного ефекту. Але, упроваджуючи СЕД не можна забувати про безпеку системи. Однією з найважливіших вимог до будь-якої СЕД є забезпечення безпеки електронного обміну документами.

У даний час все більшого поширення набувають системи захищеного електронного документообігу (ЗЕД). Це пов'язано із збільшенням кількості конфіденційних документів в органах державної влади і організаціях різної форми власності і активним переходом систем документообігу до електронного вигляду.

Підхід до захисту електронного документообігу повинен бути комплексним. Необхідно чітко оцінювати можливі загрози і ризики СЕД і можливі втрати від реалізованих загроз. Традиційний підхід до захисту інформації заснований на попередньому аналізі загроз і з'явленні їм сукупності механізмів захисту.

Основні загрози для систем електронного документообігу можуть бути класифіковані таким чином [1]:

– загроза цілісності – це пошкодження, знищення або спотворення інформації, що може бути як ненавмисним, так і зловмисним;

– загроза конфіденційності – це будь-яке порушення конфіденційності, в тому числі крадіжка, перехоплення інформації і т.д.;

– загроза працездатності системи – це загроза, реалізація якої призводить до порушення або припинення роботи системи;

– неможливість доказу авторства – це загроза, що виражається у тому, що якщо в документообігу не використовується електронний цифровий підпис, то неможливо доказати, що саме даний користувач створив даний документ (неможливо зробити документообіг юридично значимим);

– загроза доступності – це загроза, що порушує можливість отримати потрібну інформацію користувачам, що мають право доступу до неї.

Захист саме від цих загроз в тій чи іншій мірі повинна реалізовувати будь-яка система електронного документообігу. Відповідно, в комплекс захисту електронної документації повинні входити наступні заходи [2]:

– обмеження прав фізичного доступу до об'єктів СЕД;

– розмежування прав доступу до файлів і папок;

– підтвердження авторства електронного документу;

– контроль цілісності електронного документу;

– конфіденційність електронного документу;

– забезпечення юридичної сили електронного документу;

– забезпечення надійності функціонування технічних засобів;

– забезпечення резервування каналів зв'язку;

– резервне дублювання інформації;

– захист від вірусів;

– захист від "злому" мереж.

У основі реалізації захисту даних методом управління доступом лежать поняття ідентифікації і аутентифікації: ідентифікація користувача – це привласнення йому унікальних параметрів; аутентифікація – встановлення достовірності суб'єкта.

Система ідентифікації і аутентифікації користувачів є невід'ємним і важливим елементом системи захищеного електронного документообігу.

Можна констатувати, що загальними задачами для організації ЗЕД на основі систем ідентифікації і аутентифікації є: жорстка ідентифікація і аутентифікація користувачів для організації доступу до інформаційно важливих ресурсів, що захищаються; обмеження доступу до конфіденційної інформації і персональних даних; блокування несанкціонованого доступу; забезпечення доступності публічної інформації.

Тут необхідно загострити увагу на методах ідентифікації і аутентифікації користувачів комп'ютерних систем. Найпоширеніший з них, звичайно, паролний. Головна перевага паролної ідентифікації – це простота реалізації й використання. Основні проблеми, які сильно знижують надійність даного способу – це людський чинник. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. Тому деякі фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів.

Апаратний (електронний) принцип ідентифікації ґрунтується на визначенні особи користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (проксиміті-карти, смарт-карти, магнітні карти і т.д.) та так звані токени (token), які підключаються безпосередньо до одного з портів комп'ютера. Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. Але серйозною небезпекою у випадку використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані.

Максимально надійний спосіб ідентифікації і аутентифікації – біометричний, при якому користувач ідентифікується за своїми біометричними даними (це може бути відбиток пальця, сканування сітківки ока, голос і т.д.). Проте в цьому випадку вартість рішення вища, а сучасні біометричні технології ще не настільки досконалі, щоб уникнути помилкових спрацьовувань або відмов.

Ще один важливий параметр ідентифікації і аутентифікації – кількість факторів, що враховуються. Тобто, цей процес може бути однофакторним або багатфакторним, коли для визначення особи користувача

застосовується відразу кілька параметрів [3]. Також можливе комбінування різних методів: парольного, апаратного і біометричного. Втім, сьогодні найчастіше використовується тільки одна пара: парольний захист і токен. Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим суттєво підвищує рівень безпеки і захисту систем електронного документообігу.

Список використаних джерел

1. Досмухамедов Б.Р. Анализ угроз информации систем электронного документооборота // Компьютерное обеспечение и вычислительная техника. – 2009. – № 6. – С. 140-143.
2. Сабанов А.А. Некоторые аспекты защиты электронного документооборота // Connect! Мир связи. – 2010. – № 7. – С. 62-64.
3. Шпракко В.Н. Комбинированные системы идентификации и аутентификации // PCWeek/RE. – 2004. – №45. – С. 30-32.

ФРАКТАЛЬНІ ВЛАСТИВОСТІ ТРИКУТНИКА ПАСКАЛЯ

Марчук В.О., студентка,

Марач Віктор Сільвестрович, кандидат фізико-математичних наук, доцент

Рівненський державний гуманітарний університет

Робота присвячена розкриттю фрактальних властивостей трикутника Паскаля та встановленню взаємозв'язків між ними. А також наведено комп'ютерну програму для такого дослідження.

Ключові слова: фрактали, трикутник Паскаля, самоподібність у фракталах.

The work is devoted to disclosure triangle fractal properties of Pascal and establish relationships between them. A computer program is also included for this study.

Keywords: fractals, Pascal's Triangle, self-similarity of fractals.

У сучасному світі все стрімко змінюється. Це стосується і найстарішої науки – математики. На уроках геометрії ми вивчаємо кола, паралелограми, трикутники, квадрати і багато інших геометричних фігур. Проте в природі здебільшого об'єкти «неправильні» – зазубрені, поїдені ходами і отворами.



Рис. 1.1. Фрактал

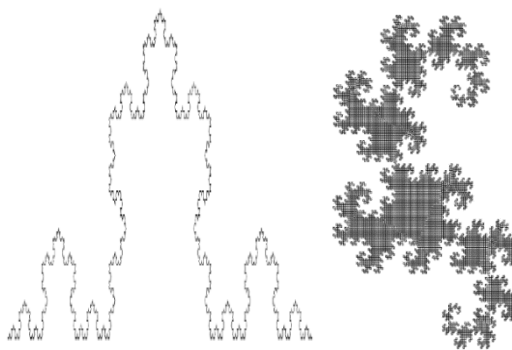


Рис. 1.2. Крива Коха та Крива «Дракона»

Перш за все, фрактали – область дивного математичного мистецтва, коли за допомогою простих формул і алгоритмів утворюються картини надзвичайної краси і складності. У контурах побудованих зображень часто вгадуються листя, дерева і квіти. (лат. fractus – подрібнений, дробовий) – нерегулярна, самоподібна структура. У широкому розумінні фрактал означає фігуру, малі частини якої в довільному збільшенні є подібними до неї самої (рис.1.1). Об'єкти, які тепер називаються фракталами, досліджувались задовго до того, як їм було дано таку назву.

На даний час виділено три класи фракталів.

1. Геометричні фрактали. Фрактали цього класу самі наочні. У двомірному випадку їх отримують за допомогою ламаної (або поверхні в тривимірному випадку), званої генератором. За один крок алгоритму кожен з відрізків, що складають ламану, замінюється на ламану-генератор у відповідному масштабі. В результаті нескінченного повторення цієї процедури виходить геометричний фрактал. Приклади геометричних фракталів наведені на (рис. 1.2).

2. Алгебраїчні фрактали. Свою назву вони отримали за те, що їх будують на основі алгебраїчних формул, іноді вельми простих. Методів отримання алгебраїчних фракталів декілька. Один з методів являє собою багаторазовий (ітераційний) розрахунок функції:

$Z_{n+1} = f(Z_n)$, де Z – комплексне число, а f – якась функція.

Наукове видання

МАТЕРІАЛИ
IX Всеукраїнської
науково-практичної конференції
„ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В
ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ»

25 березня 2015 року
м. Рівне

Відповідальний за випуск – Войтович І.С.
Комп’ютерна верстка – Гнедко Н.

Формат 60*84/16. Папір офсетний. Гарнітура Times New Romans.
Друк різнографний. Тираж прим. 120 Зам №_____

Редакційно-видавничий відділ РДГУ
вул.С.Бандери, 12, м. Рівне, 33000